

# **CITY OF SAN ANTONIO**

## **FIRE DEPARTMENT**

### **GENERAL ORDER**

**TO:** All Fire Department Personnel Sequence# G03001

**FROM:** Robert Ojeda, Fire Chief

**COPIES:** File

**SUBJECT:** Patient Access, Accounting, Amendment and Restriction on the Use of PHI

**DATE:** April 24, 2003

#### **.01 PURPOSE**

Under Standards for Privacy of Individually Identifiable Health Information, 45 CFR, Parts 160 and 164 (the Privacy Rule), individuals have the right to access and to request accounting, amendment or restriction on the use of their protected health information, or PHI. To ensure that the San Antonio Fire Department only releases PHI in accordance with the Privacy Rule, this policy shall establish the procedure by which patients or appropriate requestors may access PHI, request amendment to PHI, request accounting of uses and disclosures of PHI, and request a restriction on the use of PHI.

#### **.02 POLICY**

It is the policy of the San Antonio Fire Department to:

- A. Ensure, to the extent required by law, the confidentiality of protected health information (PHI) contained within the Designated Record Sets (DRS), as outlined in this policy.
- B. Provide notice of the privacy practices of the Department to patients, or other appropriate requestors, who request access to, amendment of and restriction on the use of their protected health information, in accordance with the Privacy Rule.
- C. Acquire patient authorization prior to use or disclosure of protected health information (PHI) for purposes other than that of treatment, payment or health care operations. Use and disclosure of protected health information (PHI) may be permitted without prior consent when:
  - 1. It is an emergency.
  - 2. A provider is required by law to treat the individual.
  - 3. There are substantial communication barriers.

### **.03 DEFINITIONS**

- A. "Employee" shall mean all personnel, both uniform and civilian, who deal with protected health information during the course of their assigned duties.
- B. "Designated Records Sets (DRS)" shall mean medical records that are created or used by the Department to make decisions about the patient (see Section .05).
- C. "Medical Records Office" shall be located at the Personnel Services Office, or other locations as designated by the Department HIPAA Privacy Officer.
- D. "Privacy Officer" shall mean that individual designated to implement the provisions of Standards for Privacy of Individually Identifiable Health Information, 45 CFR, Parts 160 and 164 (See Section .04).
- E. "Protected Health Information (PHI)" shall mean information that is a subset of health information, including demographic information collected from an individual, and:
  - 1. Is created or received by a health care provider
  - 2. Relates to the past, present or future physical or mental health condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, and:
    - a. That identifies the individual
    - b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

### **.04 PRIVACY OFFICER**

Standards for Privacy of Individually Identifiable Health Information, 45 CFR, Part 164.530 (a)(1)(i), require the San Antonio Fire Department to designate a Department HIPAA Privacy Officer. The District Chief of Personnel Services, or their designated representative, shall carry out the job duties and functions required of the HIPAA Privacy Officer.

### **.05 USE AND DISCLOSURE OF PHI WITHOUT PATIENT AUTHORIZATION**

The San Antonio Fire Department is permitted to use PHI *without* written authorization, or opportunity to object in certain situations, including, but not limited to:

- A. Use in treating an individual or in obtaining payment for services provided to the individual or in other health care operations.
- B. For the treatment activities of another health care provider;
- C. To another health care provider (such as the hospital to which an individual is transported) for the health care operations activities of the entity that receives the information as long as the entity receiving the information has or has had a relationship with the individual and the PHI pertains to that relationship;
- D. To a family member, relative, close personal friend or other individual involved in the care of the patient if the Department obtains the patient's verbal agreement to do so or if the Department gives the patient an opportunity to object to such a disclosure and the patient does not raise an objection.

- E. To the family, relatives, or friends of a patient if we can infer from the circumstances that the patient would not object.
- F. In situations where the patient is not capable of objecting (because they are not present or due to their incapacity or medical emergency), the Department may, in its professional judgment, determine that a disclosure to the patient's family member, relative, or friend is in the best interest of the patient. In that situation, the Department will disclose only health information relevant to that person's involvement with the care of the patient.
- G. To a public health authority in certain situations (such as reporting a birth, death or disease as required by law, as part of a public health investigation, to report child or adult abuse or neglect or domestic violence, to report adverse events such as product defects, or to notify a person about exposure to a possible communicable disease as required by law).
- H. For health oversight activities including audits or government investigations, inspections, disciplinary proceedings, and other administrative or judicial actions undertaken by the government (or their contractors) by law to oversee the health care system.
- I. For judicial and administrative proceedings as required by a court or administrative order, or in some cases in response to a subpoena or other legal process.
- J. For law enforcement activities in limited situations.
- K. For military, national defense and security and other special government functions.
- L. For workers' compensation purposes, and in compliance with workers' compensation laws.
- M. To coroners, medical examiners, and funeral directors for identifying a deceased person, determining cause of death, or carrying on their duties as authorized by law.
- N. If the patient is an organ donor, the Department may release health information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ donation and transplantation.

#### **.06 USES AND DISCLOSURES OF PHI WHICH REQUIRE AUTHORIZATION**

The San Antonio Fire Department, except as described in Section .05, will not use or disclosure protected health information (PHI) without the written authorization of the individual who is the subject of the PHI. The authorization must specifically identify:

- A. The information to be used and/or disclosed.
- B. When the information will be used and/or disclosed.
- C. How the Department will use or disclose it.

#### **.07 REVOCATION OF PATIENT AUTHORIZATION**

An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that the Department has already used or disclosed the protected health information in reliance on that authorization.

#### **.08 ACCOUNTING OF THE DISCLOSURE OF PHI**

The individual who is the subject of the protected health information (PHI) has a right to receive an accounting of disclosures of that PHI made by the San Antonio Fire Department in the six (6) years prior to the date on which the accounting is requested. This does not include disclosures made:

- A. To carry out treatment, payment or health care operations.

- B. To the individual who is the subject of the PHI.
- C. Pursuant to an authorization.
- D. To persons involved in the individuals care.
- E. For national security or intelligence purposes.
- F. To correctional institutions or law enforcement officials.
- G. That occurred prior to the compliance date.

The San Antonio Fire Department shall maintain an accounting log for disclosures of PHI. This accounting log will include, but not be limited to, the following information:

- A. The date of the disclosure.
- B. The name of each person or entity to whom the protected health information was given.
- C. The address of each person or entity to whom the protected health information was given.
- D. A brief description of the protected health information disclosed.
- E. A statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure (a copy of the written request for disclosure may be used in-lieu of this statement).

The San Antonio Fire Department will respond to a request for an accounting of disclosure of protected health information no later than sixty (60) days after receipt of such a request. The guidelines for providing an accounting of PHI will be as follows:

- A. The Department will provide the first accounting of disclosure of PHI to an individual in any twelve (12) month period free of charge.
- B. The Department may impose a reasonable, cost based, fee for each subsequent request for an accounting by the same individual within the twelve (12) month period, provided that the Department informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent request in order to avoid or reduce the fee.
- C. If the Department is unable to provide the accounting within the specified time frame, the Department may extend the time to provide the accounting by no more than thirty (30) days, provided that:
  - 1. The Department, within the original sixty (60) day time frame, provides the individual with a written statement of the reasons for the delay and the date by which the Department will provide the accounting.
  - 2. The Department will have only one (1) such extension of time for action on a request for accounting.

#### **.09 DESIGNATED RECORD SETS (DRS)**

The Designated Record Set for any requests for access to PHI shall include the following records:

- A. The patient care report (PCR) created by San Antonio Fire Department personnel (this includes any photographs, monitor strips, Physician Certification Statements, Refusal of Care forms), or other source data that is incorporated and/or attached to the PCR.
- B. The electronic claims records or other paper records of submission of actual claims to Medicare or other insurance companies.

- C. Any patient-specific claim information, including responses from insurance payers, such as remittance advice statements, Explanation of Medicare Benefits (EOMBs), charge screens, patient account statements, and signature authorization and agreement to pay documents.
- D. Amendments to PHI, or statements of disagreement by the patient requesting the amendment when PHI is not amended upon request, or an accurate summary of the statement of disagreement.

#### **.10 PATIENT ACCESS TO DESIGNATED RECORD SETS**

The procedure for patient (or appropriate representative) access to protected health information (PHI) shall be as follows:

- A. Upon presentation to the San Antonio Fire Department Medical Records Office, the patient or appropriate representative will complete a Request for Access Form.
- B. If the patient or patient representative is requesting an alternative method to access or obtain medical record information, or protected health information (PHI), please refer to the Procedure for Alternative Methods of Confidential Communication of Medical Information (Section .09).
- C. Authorized Department employees must verify the patient's identity, and if the requestor is not the patient, but instead is an appropriate representative, ask for legal proof of their representative status. The employee must document the name of the individual and reason that the request is being made by this individual. The use of a driver's license, social security card, or other form of government-issued identification is acceptable for this purpose.
- D. In the event that the identity and legal authority of an individual or entity requesting PHI cannot be verified, personnel will refrain from disclosing the requested information and will immediately forward the matter to the Department HIPAA Privacy Officer for a determination.
- E. The Department HIPAA Privacy Officer will act upon the request within no more than 30 days. Generally, the Department must respond to requests for access to PHI within 30 days of receipt of the access request, unless the designated record set is not maintained on site, in which case the response period may be extended to 60 days.
- F. If the Department is unable to respond to the request within these time frames, the requestor must be given a written notice no later than the initial due date for a response, explaining why the Department could not respond within the time frame and in that case the Department may extend the response time by an additional 30 days.
- G. Upon approval of access, patient will have the right to access the protected health information (PHI) contained in the Designated Record Set (DRS) outlined below and may make a copy of the protected health information (PHI) contained in the Designated Record Set (DRS) upon written request.
- H. Patient access may be denied for the reasons listed below (see Section .07, Reasons to Deny Access to PHI). In those cases the denial of access may be appealed to the Department for review.
- I. Copies of the records should be provided for the patient or requestor to view in a confidential area under the direct supervision of a designated Department staff member. The patient or patient representative may view the original Designated Record Set (DRS) only while in the Medical Records Office.

**NOTE: UNDER NO CIRCUMSTANCES SHOULD ORIGINALS OF PHI LEAVE THE PREMISES.**

- J. If the patient or requestor would like to retain copies of the Designated Record Set (DRS) provided, then the Department may charge a reasonable fee for the cost of reproduction. The Medical Records Office in conjunction with the Fiscal Management and Research Section will establish a reasonable charge for copying PHI for the patient or appropriate representative.
- K. Whenever a patient or requestor accesses a DRS, the following information must be documented:
  - 1. The name, address and phone number of the person requesting access.
  - 2. The time and date of the request.
  - 3. The date access was provided.
  - 4. What specific records were provided for review.
  - 5. A description of all copies authorized to be taken by the patient or requestor.
  - 6. The purpose of the disclosure or copy of the request for disclosure.
- M. Following a request for access to PHI, a patient or requestor may request an amendment to his or her PHI, and/or request restriction on its use in some circumstances.

**NOTE: The San Antonio Fire Department is not required to agree to any amendments and/or restrictions you request, but any amendments and/or restrictions agreed to by the San Antonio Fire Department are binding on San Antonio Fire Department.**

#### **.11 REASONS TO DENY ACCESS TO PHI**

- A. The following are reasons to deny access to PHI which are not subject to review and may not be appealed by the patient:
  - 1. If the Department was acting, in whole or in part, at the direction of a correctional institution, an inmates request for a copy of protected health information (PHI) may be denied if obtaining such a copy would jeopardize the health , safety, security, custody or rehabilitation of the individual or other inmates, or the safety of an officer, employee or other person at the correctional institution, or who is responsible for transporting the inmate.
  - 2. If the information the patient requested was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.
- B. The following reasons to deny access to PHI are subject to review and the patient may appeal the denial:
  - 1. If a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
  - 2. If the protected health information makes reference to another person (other than a health care provider) and a licensed health professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to that person.
  - 3. If the request is made by the individuals personal representative, and a licensed health care professional has determined, in the exercise of professional judgment, that provision of access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.

- C. If the denial of the request for access to protected health information (PHI) is for reasons cited in B, above, then the patient may request a review of the denial of access by sending a written request to the Department HIPAA Privacy Officer. All decisions for denial of access based on reasons A or B above must receive Executive Staff approval.
- D. The Department or City of San Antonio will designate a licensed health professional, who was not directly involved in the denial, to review the decision to deny the patient access. The Department will promptly refer the request to this designated review official. The review official will determine within a reasonable period of time whether the denial is appropriate. The Department will provide the patient with written notice of the determination of the designated reviewing official.
- E. The patient may also file a complaint in accordance with the Procedure for Filing Complaints About Privacy Practices to the Department of Health and Human Services if the patient is not satisfied with the Department or City of San Antonio's determination.

## **.12 REQUEST FOR AMENDMENT OF PHI**

An individual has the right to amend his/her patient care records, as long as his/her protected health information is maintained by the San Antonio Fire Department, except in the following circumstances:

- A. The information the patient is requesting to amend was not created by the San Antonio Fire Department.
- B. The information is not part of the patient care record.
- C. The information is accurate and complete.
- D. The information would not be available for inspection as provided by law, and therefore the San Antonio Fire Department is not required to consider an amendment. This exception applies to information compiled in anticipation of a legal proceeding.
- E. Information received from someone else under a promise of confidentiality.

The procedure to request amendment of PHI is as follows:

- A. Confirm the identity of requestor or legal representative. If the requestor is a legal representative, ask for legal proof of their representative status;
- B. The patient must fill out the Patient Request for Amendment of Protected Health Information form completely;
- C. The Department, with the assistance of legal counsel and Executive Staff will act on the request for amendment within 60 days of the request;
- D. If the Department agrees with the amendment,
  - 1. Then the record will be amended;
  - 2. The Department will then notify the individual of the agreement to amend the record;
  - 3. Copies of the amended record will be provided to San Antonio Fire Department business associates, facilities to or from which the patient was transported, and others involved in the patient's treatment.
- E. If the Department denies the request for amendment:

1. Then the individual that requested the amendment will be notified of the denial in writing, and the reason for the denial;
  2. A statement will be given to the individual that he/she may submit a short written statement disagreeing with the denial, and how the individual may file such a statement;
  3. A statement will be given to that individual that he/she may, if he/she does not wish to submit a statement of disagreement, request that the Request for Amendment and the denial become a permanent part of their medical record;
  4. A statement that the individual may complain to the Department HIPAA Privacy Officer, or to the federal agency that oversees enforcement of the federal Privacy Rule, the Department of Health and Human Services.
- F. All documentation pertaining to the request for amendment will be kept as part of the Designated Record Set (DRS).

### **.13 ALTERNATIVE METHODS FOR CONFIDENTIAL COMMUNICATION OF PHI**

The San Antonio Fire Department will take necessary steps to accommodate reasonable requests by individuals to receive confidential communications of protected health information (PHI). In complying with requests, the Department will provide confidential communications by alternative means or at alternative locations. The procedure for requesting confidential communications of protected health information (PHI) is as follows:

- A. The Department will require individuals to make a request for a confidential communication in writing.
- B. The Department will not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.
- C. When appropriate, the Department may condition the provision of a reasonable accommodation on information as to how payment, if any, will be handled, and specification of an alternative address or other method of contact.
- D. An alternative means or location will be designated on a case-by-case basis that is satisfactory to both the Department and the individual before communication of PHI is made.
- E. The Department HIPAA Privacy Officer, using professional judgment and considering all relevant factors, will be responsible for deciding the alternative means or location to communicate PHI to an individual.
- F. Once it is determined that use or disclosure is appropriate, personnel with appropriate access clearance will access the individual's PHI using proper access and authorization procedures.
- G. The requested PHI will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
- H. Copies of the records will be provided for the patient or requestor to view in a confidential area under the direct supervision of a designated Department staff member.
- I. Department personnel will appropriately document the request and delivery of the PHI.
- J. In the event that the identity and legal authority of an individual or entity requesting PHI cannot be verified, Department personnel will refrain from disclosing the requested information and report the case to the Department HIPAA Privacy Officer in a timely manner.

#### **.14 PERSONAL REPRESENTATIVES**

The San Antonio Fire Department will treat personal representatives the same as the individual who is the subject of the protected health information. If, under applicable law, a person has authority to act on behalf of an individual who is an adult, or an emancipated minor, in making decisions related to health care, the Department will treat that person as the personal representative.

#### **.15 MINORS**

If, under applicable law, a parent, guardian or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, the San Antonio Fire Department will treat that individual as a personal representative with respect to protected health information relevant to such representation.

The individual may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual with respect to protected health information pertaining to a health care service if:

- A. The minor consents to such health care service; no other consent is required by law, regardless if the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative.
- B. The minor may lawfully obtain such health care service without the consent of a parent, guardian or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service.
- C. A parent, guardian or other person acting *in loco parentis* assents to an agreement of confidentiality between the San Antonio Fire Department and the minor with respect to such health care service.

#### **.16 DISCLOSURE OF PHI CONCERNING DECEDENTS**

The San Antonio Fire Department may disclose protected health information (PHI) to coroners, medical examiners, funeral directors and organ procurement organization pursuant to applicable law. The procedure for disclosure of a decedent's PHI is as follows:

- A. The San Antonio Fire Department may disclose PHI about a deceased person, without individual authorization, to coroners, medical examiners, funeral directors or organ procurement organizations for the following purposes:
  - 1. The Department may disclose PHI to coroners or medical examiners to identify a deceased person, determining a cause of death, or other duties as authorized by law.
  - 2. The Department may disclose PHI to assist funeral directors, in carrying out their duties with respect to the decedent including, if necessary, disclosing PHI prior to, and in reasonable anticipation of, the individual's death.
  - 3. The Department may disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking or transplantation of cadaveric organs, eyes or tissue for the purpose of facilitating organ, eye and tissue donation and transplant.

- B. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting PHI (see Section .06 Patient Access to Designated Records Sets).
- C. Once it is determined that use or disclosure is appropriate, medical records personnel with appropriate access clearance will access the individual's PHI using proper access and authorization procedures.
- D. The requested PHI will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
- E. Medical records personnel will appropriately document the request and delivery of the PHI.
- F. In the event that the identity and legal authority of an individual or entity requesting PHI cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Department HIPAA Privacy Officer in a timely manner.
- G. Knowledge of a violation or potential violation of this policy must be reported directly to the Department HIPAA Privacy Officer.

### **.17 DISCLOSURE OF PHI TO A HEALTH OVERSIGHT COMMITTEE**

The San Antonio Fire Department may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings, except as otherwise stated in this policy and procedure.

If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits unrelated to health, the Department considers the joint activity or investigation to be a health oversight activity.

The Department will not disclose PHI without authorization in cases where an individual is the subject of the investigation or other activity, if such investigation or other activity does not arise out of and is not directly related to:

- A. The receipt of health care;
- B. A claim for public benefits related to health;
- C. Qualification for or receipt of public benefits or services when a patient's health is integral to the claim for public benefits or services.

The San Antonio Fire Department may disclose PHI to a health oversight agency under the following guidelines:

- A. The Department may disclose PHI without authorization to a health oversight agency if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health.
- B. Personnel receiving a request from an individual or entity for use or disclosure of PHI will utilize the Department's access control system to determine whether the requesting individual is a person whom the Department has a knowing relationship.
- C. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting PHI (see Section .06 Patient Access to Designated Records Sets).

- D. Once it is determined that use or disclosure is appropriate, medical records personnel with appropriate access clearance will access the individual's PHI using proper access and authorization procedures.
- E. The requested PHI will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
- F. Medical records personnel will appropriately document the request and delivery of the PHI.
- G. In the event that the identity and legal authority of an individual or entity requesting PHI cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Privacy Officer in a timely manner.
- H. Knowledge of a violation or potential violation of this policy must be reported directly to the Privacy Officer.

## **.18 SPECIALIZED GOVERNMENT FUNCTIONS**

The San Antonio Fire Department may use or disclose protected health information for the following specialized government functions:

- A. Armed Services Personnel – The Department may use or disclose protected health information (PHI) of individuals who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the appropriate military authority has published by notice in the **Federal Register** the following information:
  - 1. Appropriate military command authorities
  - 2. The purpose for which the PHI may be used or disclosed.
- B. Foreign Military Personnel – The Department may use or disclose PHI of individuals who are foreign military personnel to their appropriate military authority for the same purposes for which uses and disclosures are permitted for Armed Forces personnel under the notice published in the **Federal Register**.
- C. National Security and Intelligence Activities – The Department may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence and other national security activities authorized by the National Security Act
- D. Protective Services for the President - The Department may disclose PHI to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709 (a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879.
- E. Correctional Institutions and Other Law Enforcement Custodial Situations – The Department may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individuals PHI about such inmate or individual, if the correctional institution or such law enforcement official represents that such PHI is necessary for:
  - 1. The provision of health care to such individuals.
  - 2. The health and safety of such individual or other inmates.
  - 3. The health and safety of the officers or employees of or others at the correctional institution.
  - 4. The health and safety of such individuals and officers or other individuals responsible for the transporting of inmates or their transfer from one institution, facility or setting to another.
  - 5. Law enforcement on the premises of the correctional institution.

6. The administration and maintenance of the safety, security and good order of the correctional institution.

#### **.19 DISCLOSURE OF PHI FOR JUDICIAL OR ADMINISTRATIVE PROCEEDINGS**

The San Antonio Fire Department may disclose PHI pursuant to a judicial or administrative process without the written consent or authorization of the individual, or the opportunity for the individual to agree or object, in situations subject to the applicable requirements of 45 CFR §164.512. To support the San Antonio Fire Department's commitment to patient confidentiality, the Department will ensure any use or disclosure of PHI for judicial and/or administrative release is in compliance with all applicable laws and regulations.

The San Antonio Fire Department will comply with all lawful and appropriate requests from regulatory and judicial authorities and may disclose PHI necessary in response to:

- A. A subpoena, grand jury subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal;
- B. A subpoena, discovery request, or other lawful process that is accompanied by an order of a court or administrative tribunal.

Disclosures will be made of only that PHI that is expressly authorized in an appropriate request, such as in response to a subpoena, discovery request, or other lawful process that is not accompanied by an order of a court or administrative tribunal. The procedure for disclosure of PHI pursuant to a judicial or administrative process is as follows:

- A. The Department will disclose PHI only after obtaining satisfactory assurance from the requesting party that they have made reasonable efforts to provide notice to the individual who is the subject of the requested PHI or to secure a qualified protective order.
- B. The Department will obtain a written statement and accompanying documentation demonstrating that a notice has been given to the individual that contained sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal.
- C. Where reasonable efforts have been made to ensure that the individual has been given notice of the request, the Department will obtain from the requesting party a written statement and accompanying documentation demonstrating that:
  1. Time for raising objections to the court or administrative tribunal has elapsed, and
  2. No objections were filed, or
  3. The court has resolved all objections filed by the individual or the administrative tribunal and the disclosures being sought are consistent with such resolution.
- D. Where reasonable efforts have been made to secure a qualified protective order, the Department will obtain from the requesting party a written statement and accompanying documentation demonstrating that:
  1. Parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute, or

2. Party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.
- E. Personnel receiving a request from an individual or entity for use or disclosure of PHI will utilize the Department's access control system to determine whether the Department has a knowing relationship with the requesting individual.
- F. Personnel will follow appropriate policies and procedures for verifying the identity and authority of individuals requesting PHI (see Section .06 Patient Access to Designated Records Sets).
- G. Once it is determined that use or disclosure is appropriate, medical records personnel with appropriate access clearance will access the individual's PHI using proper access and authorization procedures.
- H. The requested PHI will be delivered to the individual in a secure and confidential manner, such that the information cannot be accessed by employees or other persons who do not have appropriate access clearance to that information.
- I. Medical records personnel will appropriately document the request and delivery of the PHI.
- J. In the event that the identity and legal authority of an individual or entity requesting PHI cannot be verified, personnel will refrain from disclosing the requested information and report the case to the Department HIPAA Privacy Officer in a timely manner.
- K. Knowledge of a violation or potential violation of this policy must be reported directly to the Department HIPAA Privacy Officer.

## **.20 PUBLIC HEALTH AND SAFETY CONCERNS**

The San Antonio Fire Department may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the Department, in good faith, believe that use or disclosure :

- A. Is necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public; and
- B. Is to a person or persons is reasonably able to prevent or lessen the threat, including the target of the threat; or
- C. Is necessary for law enforcement authorities to identify or apprehend an individual:
  1. Because of a statement by an individual admitting to participation in a violent crime that the Department reasonably believes may have caused serious physical harm to the victim; or
  2. Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

## **.21 DE-IDENTIFICATION OF PHI**

Federal law allows certain health care organizations to use or disclose protected health information (PHI) for the purpose of creating de-identified information, that is, information that has been stripped of any elements that may identify the patient, such as name, birth date, or social security number. The San Antonio Fire Department will, from time to time, use de-identified data for various purposes such as utilization research. In doing so, the San Antonio Fire Department will ensure that the appropriate administrative and technical processes are in place to properly de-identify PHI, as well as to secure any methods of re-identification, as

required under 45 CFR §164.514(a) and other applicable federal, state, and/or local laws and regulations.

The procedure for de-identification of PHI shall be as follows:

- A. The Department HIPAA Privacy Officer, in conjunction with Executive staff, shall make decisions as to whether PHI should be de-identified.
- B. The reason for de-identification will be documented and maintained.
- C. The following individually identifying elements will be removed or otherwise concealed from PHI in order to create de-identified information:
  - 1. Names;
  - 2. All elements of dates (except year) for dates directly related to an individual, including:
    - a. birth date
    - b. admission date
    - c. discharge date
    - d. date of death
    - e. all ages over 89
    - f. all elements of dates (including year) indicative of age 89, except that such ages and elements may be aggregated into a single category of age 90 or older;
  - 3. Telephone numbers;
  - 4. Fax numbers;
  - 5. Electronic mail addresses;
  - 6. Social security numbers;
  - 7. Medical record numbers;
  - 8. Health plan beneficiary numbers;
  - 9. Account numbers;
  - 10. Certificate/license numbers;
  - 11. Vehicle identifiers and serial numbers, including license plate numbers;
  - 12. Device identifiers and serial numbers;
  - 13. Web Universal Resource Locators (URLs);
  - 14. Internet Protocol (IP) address numbers;
  - 15. Biometric identifiers, including finger and voice prints;
  - 16. Full face photographic images and any comparable images;
  - 17. All geographic subdivisions smaller than a State, including:
    - a. street address
    - b. city county
    - c. precinct
    - d. zip code, and their equivalent geocodes
  - 18. Any other unique identifying number, characteristic, or code
  - 19. The initial three digits of a zip code may be used if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000).
- D. If any of the listed identifiers are not removed, then the information will only be disclosed when authorized personnel:

1. Determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information, and
  2. Document the methods and results of the analysis that justify such determination.
- E. Knowledge of a violation or potential violation of this policy must be reported directly to the Department HIPAA Privacy Officer.

## **.22 RE-IDENTIFICATION OF PHI**

The Department may assign codes or other means of record identification to allow information that has been de-identified to be re-identified, provided that:

- A. The code or other means of record identification used to re-identify information will not be derived from or related to information about the individual and should not otherwise be capable of being translated so as to identify the individual.
- B. The use or disclosure of the code or other means of record identification does not disclose the mechanism for re-identification.

Knowledge of a violation or potential violation of this policy must be reported directly to the Department HIPAA Privacy Officer.

## **.23 COMPLAINT PROCEDURE**

The San Antonio Fire Department is committed to the provision of the security to all patient protected health information, which is created, stored or maintained in any format regardless of location and grants each patient special rights as it pertains to their individually identifiable health information. Federal law requires the Department to provide each patient or patient representative with a method to lodge complaints or concerns regarding their patient privacy rights as granted under HIPAA. The process for handling patient privacy issues and complaints shall be as follows:

- A. Once contacted by an individual that an issue regarding patient privacy exists, the Department HIPAA Privacy Officer will become the primary contact for all communications regarding this issue.
- B. The Department HIPAA Privacy Officer will handle the patient privacy issue in the manner that best represents the needs of the patient, the Department and the City of San Antonio.
- C. The Department HIPAA Privacy Officer will inform the Legal Advisors Office in a timely manner that a complaint has been filed and an investigation regarding patient privacy has been initiated.
- D. The Department HIPAA Privacy Officer, through coordination with the Legal Advisors Office, will oversee all aspects of the investigation.
- E. The Department HIPAA Privacy Officer, will thoroughly document all aspects of the complaint.
- F. The Department HIPAA Privacy Officer will prepare a final report detailing his recommendation for resolution to the complaint, and a printed copy of the report will be attached to the patient's medical record.

- G. The Department HIPAA Privacy Officer shall complete the investigation within 30 days, and shall relay the details of the final report to the individual filing the complaint. If the individual filing the complaint is not satisfied with the outcome, the Department HIPAA Privacy Officer shall inform them of their right to seek resolution through the U.S. Department of Health and Human Services.

**NOTE: The San Antonio Fire Department shall not intimidate or retaliate against any individual, or group of individuals, choosing to file a complaint, either to the Department, or to the Secretary of the U.S. Department of Health and Human Services, as described in this Section.**

#### **.24 CONFLICT AND REVISION**

- A. Where previous correspondence conflicts with this policy, this policy shall supersede.
- B. This policy may be subject to revision as necessary to ensure efficient, thorough and logical procedures for the protection of identifiable health information that are in strict compliance with all applicable state and federal laws.

Robert Ojeda, Fire Chief  
San Antonio Fire Department